¿QUÉ HACER CUANDO EL ANTIVIRUS DEJA DE SER UN CONTROL EFECTIVO ANTE UN ATAQUE DE MALWARE?

JUAN CARLOS GAMEZ RAMIREZ
Universidad Piloto de Colombia
Bogotá, Colombia
jcgamezr@gmail.com

Resumen – Las compañías, empresas u organizaciones sin importar su tamaño, buscan preservar los tres pilares de la seguridad de la información, confidencialidad, integridad y disponibilidad. Para cumplir este objetivo, implementan controles como antivirus que permiten aumentar su nivel de seguridad. Sin embargo, cada día el malware se hace más fuerte, recursivo y en algunas ocasiones logran evadir el antivirus, convirtiéndose en una amenaza potencial, provocando fugas o eliminación de información, no disponibilidad del servicio, modificación de datos, pérdidas económicas y de reputación. El objetivo de este artículo, es validar un procedimiento que permita reaccionar de forma rápida y efectiva ante este tipo de malware.

Abstract – The company or organization regardless of the size, always treat of preserve the three pillars of information security, confidentiality, integrity and availability. To accomplish this goal, implement controls like antivirus allows them to increase their level of security. Nevertheless, every day malware becomes stronger, recursive and sometimes evades the antivirus, thus becoming a potential threat that can lead to information leakage, or deletion of information, unavailability of the service, data modification, economic loss and reputation. The objective of this article is to validate a procedure that allows to react quickly and effectively to this type of malware.

Índice de Términos – Malware, antivirus, información, confidencialidad, integridad y disponibilidad.

I. INTRODUCCIÓN

El software malicioso o malintencionado también conocido como malware por su término en inglés, corresponde a todos los programas que tienen como objetivo infiltrarse y ser indetectables en un sistema, dependiendo de las motivaciones de su creador pueden entorpecer, bloquear, dañar u otorgar acceso a una aplicación, un sistema de información, un computador, una red o sencillamente obtener un beneficio económico. Para conseguir su propósito el malware emplea alguna vulnerabilidad de sus objetivos, ganando privilegios, indicando un análisis previo, una fase de planificación y preparación antes de iniciar el ataque.

Las compañías de antivirus realizan análisis para identificar y clasificar el malware, generando y agrupando esta información en bases de datos para realizar la detección y posteriormente eliminación de archivos con contenido malicioso. Este procedimiento es vulnerable en casos relacionados con ofuscación, polimorfismo, metamorfismo y zero-day.

El desarrollo de malware ha presentado un incremento exponencial en los últimos 5 años, en gran medida a su diversificación para afectar cualquier dispositivo que pueda conectarse a internet, llegando de esta forma a casi 600 millones de programas maliciosos existentes. Como se evidencia en la figura 1, sin lugar a duda el malware se convierte en una amenaza latente que tarde o temprano los usuarios están obligados a enfrentar.

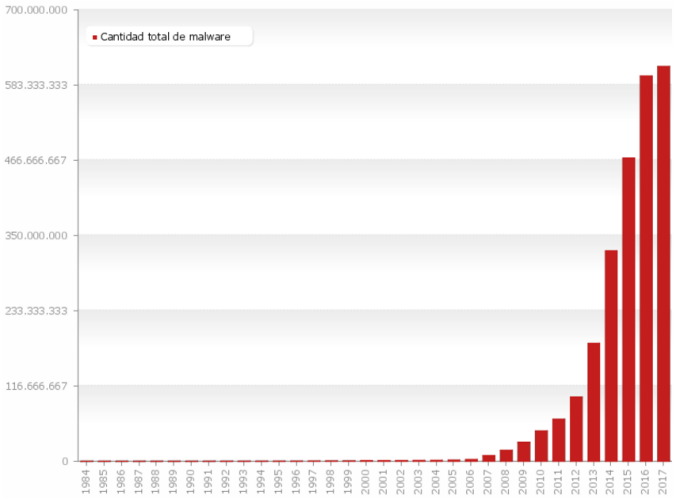

Figura 1. Estadística de malware AV-Test [1]

Los incidentes de seguridad relacionados con infección por malware cada vez son mayores, debido a al aumento en cantidad, complejidad y diversidad. Por esta razón, el 77% de las empresas en latinoamérica invierte en antivirus como un mecanismo de protección, ver figura 2.

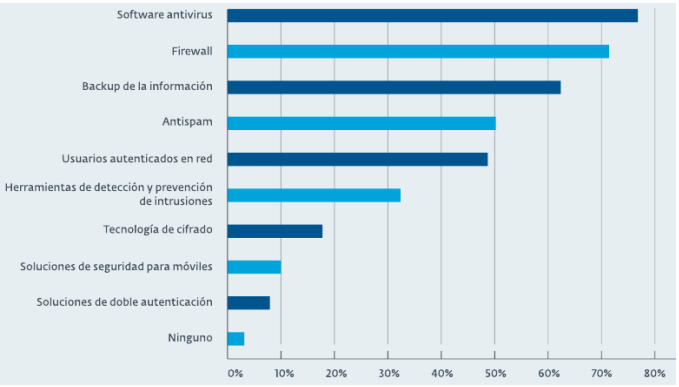

Figura 2. Implementación de controles de seguridad [2]

En algún momento las personas responsables del área de seguridad informática de la compañía, empresa u organización deben preguntarse **¿Qué hacer cuando el antivirus deja de ser un control efectivo ante un ataque de malware?** Este artículo pretende validar un procedimiento para identificar de forma rápida y efectiva las acciones correctivas necesarias y comprobar su aplicación en un caso específico.

II. CONCEPTOS PRELIMINARES

En este apartado se explican algunos conceptos fundamentales para entender el funcionamiento del malware, motivación, clasificación, métodos de infección y análisis.

A. Antivirus

Corresponde al software que tiene la misión de identificar, clasificar y eliminar cualquier tipo de malware. Se utilizan principalmente tres métodos para su clasificación:

Método basado en firmas; toma un fragmento del archivo sospechoso y le asigna una firma, luego realiza una comparación contra una base de datos compuesta por firmas de malware conocido, cuando existe una coincidencia exacta entre las firmas, el archivo es malicioso.

Método basado en comportamiento; de acuerdo a una serie de reglas que describen las acciones permitidas para los programas en ejecución, se realiza una supervisión constante del comportamiento en búsqueda de acciones inusuales, en caso de obtener algún acierto se procede a bloquear el programa.

Método heurístico; compara la correspondencia de una muestra de malware evaluando los bloques de código, el tiempo de ejecución y los requerimientos de memoria contra una base de datos de programas maliciosos.

B. Motivación del Malware

Inicialmente el objetivo del malware era otorgar protagonismo público a su creador, estos programas maliciosos se caracterizaban por su fácil visibilidad. Buscaban modificar programas, borrar información, eliminar ficheros y alterar las características del sistema. Ahora, la motivación es económica con la actual integración de internet a transacciones bancarias y comerciales, el malware se ha convertido en una fuente de ingresos rentable. Por esta razón, existen organizaciones dedicadas al desarrollo y venta de códigos maliciosos de difícil detección.

C. Métodos de infección de Malware

Usualmente el malware se instala sin autorización del usuario y la infección puede ser ocasionada por los siguientes vectores:

Archivo malicioso; el malware puede llegar como un archivo adjunto o por carpetas compartidas aprovechando la red para expandirse y replicarse.

Dispositivos extraíbles; el malware puede guardar una copia de sí mismo en este tipo de dispositivos, ejecutarse e infectar cuando se conecte nuevamente.

Instalación; es la forma más común, sucede cuando el usuario instala programas que aparentan ser legítimos y de gran funcionalidad, pero termina instalando indirectamente el malware.

Explotación de vulnerabilidades; cualquier aplicación o programa instalado en el computador es

susceptible a tener ciertas brechas de seguridad, por ejemplo, un navegador web, un cliente de correo electrónico e inclusive el sistema operativo, son vulnerables y proporcionan una puerta de entrada para instalar malware.

Ingeniería Social; su estrategia es atraer la atención del usuario y está relacionada con correos en donde se persuade al usuario a ejecutar archivos adjuntos o conectarse a páginas maliciosas por medio de links, haciéndole creer que son legítimas.

D. Clasificación del Malware

Se clasifican según los efectos que produce en:

Adware; corresponde a software publicitario que se reproduce y descarga sin consentimiento del usuario, algunas veces, redirige el navegador a páginas web de anuncios. Generalmente la publicidad que se muestra esta seleccionada de acuerdo a las posibles preferencias del usuario, estas han sido recopiladas previamente en internet o simplemente al realizar búsquedas en cualquier navegador.

Botnet; corresponde a una red de equipos infectados por malware y son controlados de forma remota por un atacante, el cual dispone de sus recursos para cualquier propósito. Cada máquina infectada se conoce como zombie.

Crimeware; corresponde al software malicioso diseñado para cometer fraude de tipo económico y financiero. Obteniendo por medio de keylogger (captura de pulsaciones del teclado) usuarios, contraseñas, números de tarjetas de crédito y cuentas bancarias para posteriormente realizar transacciones no autorizadas.

Grayware; no causan daños al equipo o la red, pero ocasionan inconvenientes como lentitud en los procesos del sistema operativo, rastreo de actividad del usuario y modificación de la página de inicio del navegador.

Gusano; se caracteriza por ser independiente, alojarse en la memoria ram y se replica rápidamente de forma automática, enviando copias de sí mismo por medio de la red a otros computadores, utilizando algunos procesos del sistema operativo.

PUA; aplicaciones potencialmente indeseadas por sus siglas en inglés, son programas maliciosos que presentan una serie de comportamientos indeseados por el usuario, entre ellos está la instalación de adware o rougeware, la activación de alertas por fallas en el registro o en el sistema operativo (falsos positivos), la instalación de barras de herramientas y la modificación en la configuración del navegador de internet. Este tipo de malware, afecta seriamente el rendimiento del equipo consumiendo recursos del procesador y memoria ram.

Ramsonware; este software malicioso pretende obtener un beneficio económico de forma rápida cifrando algunos archivos del computador, evitando que se puedan consultar, es decir, secuestran archivos y luego piden un rescate enviando un mensaje al propietario exigiendo un pago para revelar la clave de descifrado.

Rootkit; su objetivo es tener el control de un sistema operativo y proporciona acceso remoto a un atacante con los permisos y privilegios de la cuenta superusuario (root), para permanecer oculto, este malware realiza modificaciones cambiando archivos, puertos, claves de registro, directorios, procesos y ficheros.

Rougeware; es un falso antivirus que pretende engañar al usuario haciéndole creer que su computador está infectado por malware y lo induce a comprar e instalar un programa de seguridad para remediar esta situación.

Spyware; este software malintencionado recopila datos del usuario sobre búsquedas, navegación, costumbres y hábitos. La información recolectada se trasmite a una entidad externa y puede ser utilizada para realizar un ataque personalizado.

Troyano; este tipo de software se oculta en una aplicación de uso normal, aparentemente legítimo e inofensivo, pero sin conocimiento del usuario otorga acceso de forma remota a usuarios externos de la red. Depende de un agente externo para completar su objetivo y puede permitir acciones como abrir

puertos, borrar información, capturar y reenviar datos confidenciales, realizar capturas de pantalla, instalar otros programas maliciosos, etc.

Virus; su objetivo es alterar el comportamiento normal de equipo, reemplazando o modificando archivos del sistema por otros infectados, se caracterizan por ser autoreplicables y no dependen de agentes externos. Su activación puede ser por medio de un archivo autoejecutable, o cuando se cumpla una condición programada previamente.

E. Análisis de Malware

Es una labor compleja, debido a la constante evolución y recursividad del software malicioso. Su principal objetivo es comprender la estructura y funcionamiento del malware para encontrar las acciones correctivas necesarias. Eventualmente, su intención es identificar la vulnerabilidad aprovechada, evaluar los sistemas de protección y conocer el origen del ataque [3].

Existen dos tipos de análisis de malware: análisis estático y análisis dinámico. El primero, se caracteriza por ser un procedimiento rápido y sencillo que consiste en un estudio de las particularidades del software malicioso, sin la necesidad de ejecutarlo. Dentro de las actividades sugeridas se encuentran, identificación con antivirus y hash, ingeniería inversa para descubrir cadenas, librerías y vínculos a funciones. Las principales desventajas es que pueden ser ineficaces frente a malware ofuscado y omitir comportamiento importante. El segundo tipo de análisis, estudia el comportamiento del malware al ejecutarse y monitorea los recursos utilizados en el sistema operativo, las modificaciones en el registro y los ficheros afectados, utilizando herramientas como, netcat, process explorer, regshot y wireshark [4].

Actualmente, los métodos de virtualización permiten simular sistemas operativos, aplicaciones y redes; por esta razón son apropiados para realizar de forma rápida y aislada el análisis dinámico de malware. Sin embargo, reproducir virtualmente la red de una organización puede ser muy complicado, algunas variables y condiciones claves no están disponibles. En este escenario, no se puede establecer claramente cuál es el objetivo principal del código malicioso. Adicionalmente, algunas clases de malware establecen si se encuentran en una maquina física o virtual y cambian su comportamiento, logrando entorpecer el proceso de análisis.

F. Ofuscación

Esta técnica es utilizada para entorpecer el proceso de análisis, evadir la detección de antivirus y evitar la ingeniería inversa. Consiste en reemplazar partes del código por caracteres sin sentido, manteniendo la funcionalidad y el comportamiento.

G. Zero-Day

Se produce cuando un atacante aprovecha una vulnerabilidad desconocida de un sistema antes que sus propietarios la descubran. Para esta vulnerabilidad no se ha creado ninguna medida de remediación.

H. Vulnerabilidad

Se trata de una debilidad en un archivo o un sistema debido a un error en la creación o implementación y puede ser aprovechado por una amenaza.

I. Keylogger

Corresponde a software o hardware, cuya función es guardar todas las pulsaciones del teclado realizadas por el usuario, almacenarlas en un archivo log y posteriormente enviarlas al atacante.

J. Polimórfico

Este malware cifra su código con una clave variable y se carga en memoria cuando se ejecuta un archivo infectado, puede crear un número ilimitado de copias diferentes usando conjuntos aleatorios para su proceso de descifrado. Con este método oculta su presencia e impide su detección.

K. Metamórfico

Se trata de malware que tiene la capacidad de editar y reescribir su código, utilizando múltiples técnicas de transformación, cambia su estructura interna cada vez que infecta una máquina. Los cambios en el código dificultan la identificación basada en firmas.

L. Hash

Es una función unidireccional de comprobación aleatoria que reduce un conjunto de datos de entrada a una cadena alfanumérica fija e irrepetible. Se utiliza principalmente para verificar la integridad de archivos.

III. CONTEXTO

Sin importar el sector productivo donde se encuentren las organizaciones, siempre buscan preservar los pilares de la seguridad de la información. Como parte de la implementación de los controles debe ser instalado un agente antivirus en cada máquina de la red, para su control se dispone de una consola de administración. La comunicación entre el agente y la consola debe ser permanente, permitiendo el registro de las detecciones de malware a través de un log y realizando las actualizaciones de firmas por medio de paquetes.

El antivirus comienza a detectar y eliminar el malware dexon, luego informa al usuario la necesidad de proceder con el reinicio de la máquina para terminar el proceso de desinfección. Posteriormente, la maquina se vuelve a infectar y el antivirus repite el ciclo *desinfección – notificación – reinicio*.

Esta situación llega a convertirse prácticamente en una denegación de servicio, debido a que los usuarios no pueden realizar su trabajo y afecta la operación de la organización, inclusive algunas máquinas reportaron 20.000 detecciones diarias y el impacto en la red era considerablemente alto, debido al consumo de recursos para el envió de notificaciones desde el agente hacia la consola.

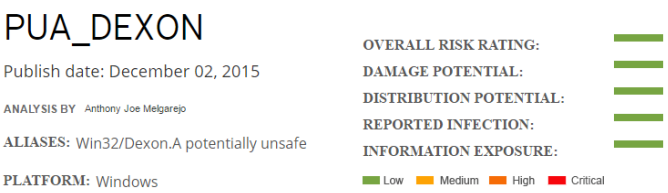

Figura 3. Análisis PUA_Dexon [5]

Reportes preliminares indicaban que el 60% de la organización estaba infectada. Al revisar un análisis propuesto por Antony Joe Melgarejo (ver figura 3), este malware está clasificado como PUA con un impacto bajo, pero con una afectación importante dentro de la organización, representando un problema serio. La categorización del malware dexon realizada por el antivirus esta sesgada y los criterios evaluados (función, distribución, impacto y utilidad) para determinar qué tan malicioso es, no refleja la realidad dentro de la organización. Aunque el antivirus identifica y elimina a dexon, por la reiterativa infección de las maquinas, se considera que este control tecnológico ha dejado de ser efectivo.

IV. ANÁLISIS DE MALWARE DEXON

De acuerdo a las características del malware dexon, el impacto ocasionado dentro de la organización y los tipos de análisis, se optó por un procedimiento alternativo de tres fases, la primera, la identificación por medio de un análisis estático, la segunda, monitoreando el comportamiento con wireshark y una maquina conectada a la red. Posteriormente, con la información recolectada, se plantean las acciones correctivas para la fase de erradicación.

A. Primera fase: identificación

Al revisar las maquinas infectadas por el malware dexon, se recopilo información relacionada con su comportamiento, se detectaron modificaciones en el registro, para garantizar su ejecución automática cada vez que inicia el sistema, ver figura 4.

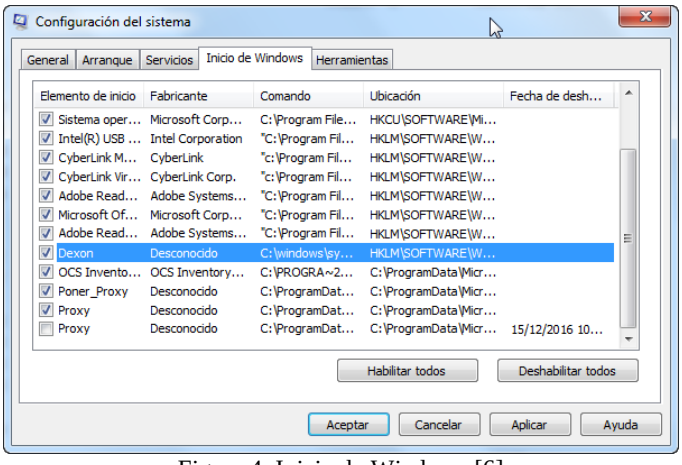

Figura 4. Inicio de Windows [6]

Así mismo, crea una carpeta dat en dos ubicaciones distintas, estas son protegidas por el sistema y copia 77 archivos, ver figura 5.

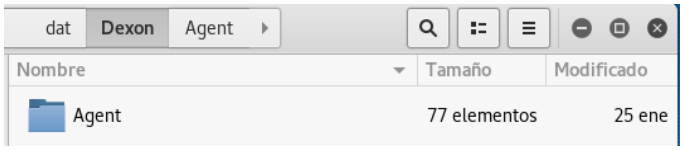

Figura 5. Carpeta dat [7]

El archivo module04.dll alojado en la carpeta dat, se verifico en la página virus total y se encontraron 18 coincidencias como archivo malicioso, ver figura 6.

Figura 6. Análisis module04.dll en virus total [8]

B. Segunda fase: monitoreo

En esta fase se dispuso de una máquina con borrado seguro para garantizar la eliminación permanente de cualquier tipo de malware. Luego, se reinstaló el sistema operativo y las aplicaciones de producción, también, se instaló wireshark para realizar el análisis dinámico. Posteriormente la maquina se conectó a la red y se comenzó con el proceso de análisis. Aunque los expertos aconsejan realizar este tipo de análisis en un entorno controlado, la organización decidió aceptar el riesgo debido al impacto ocasionado por dexon.

Dexon utiliza los puertos 445 y 6008, para descubrir y establecer comunicación con otras máquinas de la red, para esto envía un ping y realiza una negociación, ver figura 7.

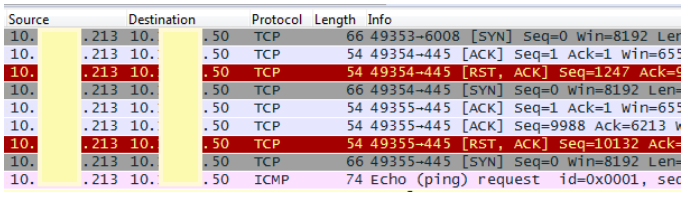

Figura 7. Análisis wireshrak de puertos utilizados por dexon [9]

En el caso que no pueda acceder a los recursos compartidos de una máquina, realiza un escaneo para encontrar la unidad de almacenamiento disponible, ver figura 8.

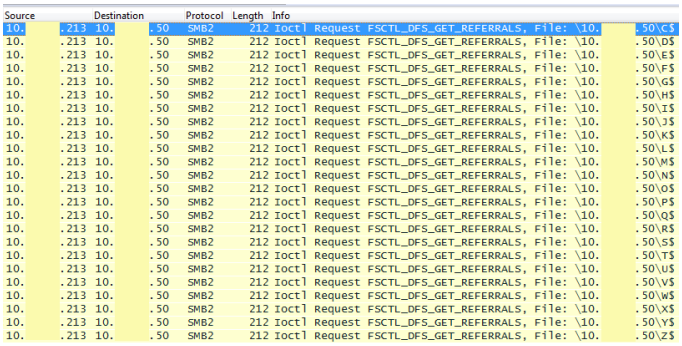

Figura 8. Escaneo de recursos compartidos [10]

Dexon se encarga de infectar a las maquinas constantemente, estableciendo comunicación con otra máquinas, y realizando un escaneo de los directorios, posteriormente copia los archivos faltantes, ver figura 9. Este ciclo genera latencia en la red y mantinene un consumo de recursos importantes, afectando el rendimiento de la organización.

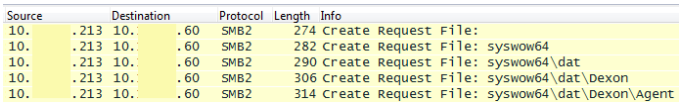

Figura 9. Copia de archivos realizados por dexon [11]

C. Tercera fase: erradicación

Después de analizar la información obtenida en las fases previas, se establecieron las siguientes acciones correctivas:

- Eliminar los recursos compartidos desde A$ hasta Z$ y ADMIN$, mantener IPC$, ver figura 10.

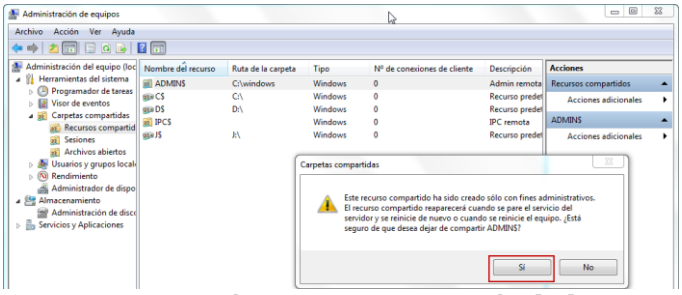

Figura 10. Eliminar recursos compartidos [12]

- Eliminar desde el firewall de Windows todas las reglas con nombre ***Dexon Agent***, ver figura 11.

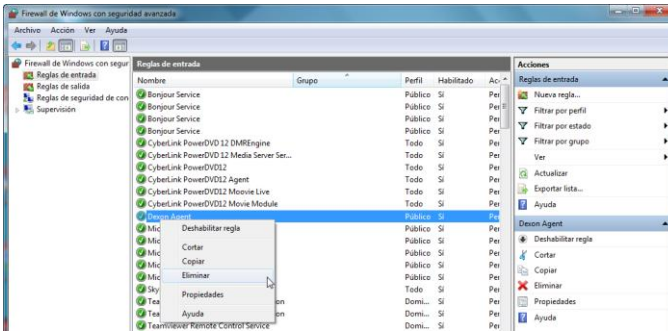

Figura 11. Eliminar reglas de firewall [13]

- Deshabilitar todas las entradas en las pestañas de inicio de windows y servicios para dexon, ver figura 12.

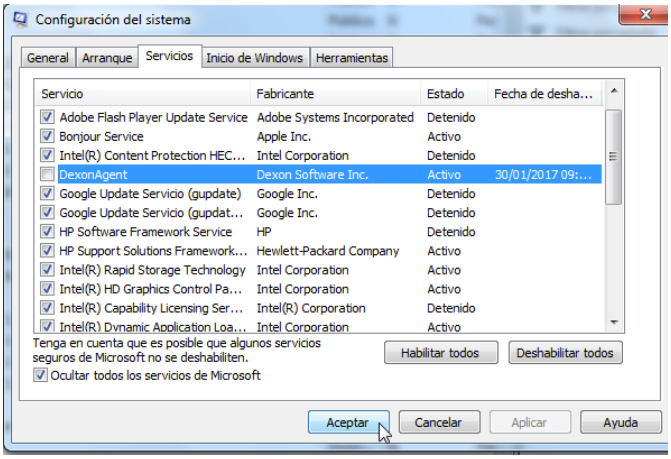

Figura 12. Deshabilitar inicio [14]

- Eliminar todas las entradas y llaves con la palabra dexon en el registro de windows, ver figura 13.

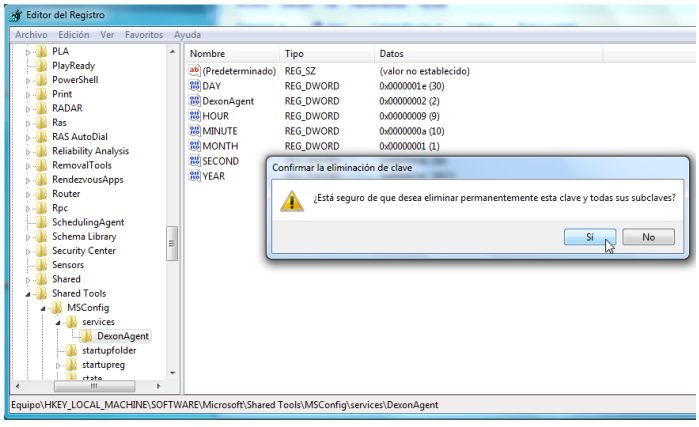

Figura 13. Eliminar llaves en el registro [15]

- Para detener el servicio *DexonAgent*, ingrese a servicios de windows, ver la figura 14.

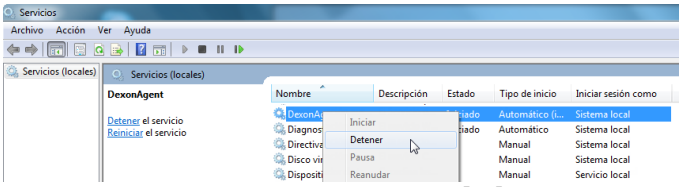

Figura 14. Detener servicio [16]

- Crear regla en el firewall de windows para el protocolo tcp y bloquear los puertos 445 y 6008, ver figura 15. También bloquear el servicio *DexonAgent*, ver figura 16.

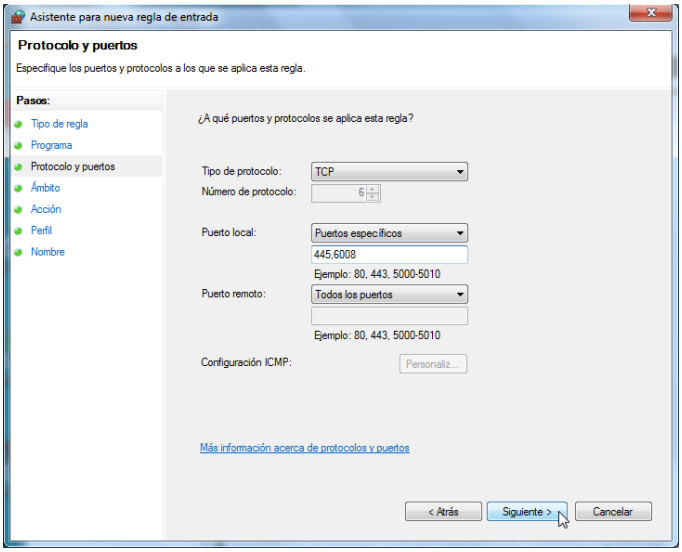

Figura 15. Regla para bloqueo de puertos [17]

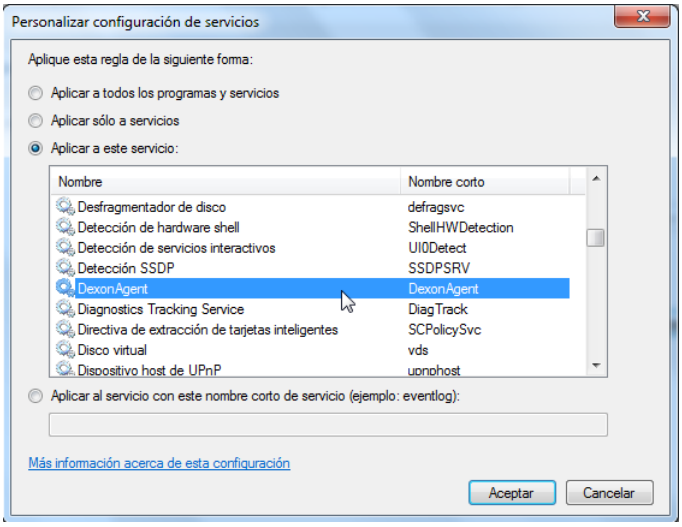

Figura 16. Regla para bloqueo de servicio [18]

Para concluir el procedimiento se debe reiniciar la máquina y verificar que las acciones correctivas estén conforme a los pasos descritos. En caso contrario es necesario realizarlo nuevamente.

VI. CONCLUSIONES

Realizar el análisis de malware tiene un valor agregado para la organización, debido a que el área de exposición ante las amenazas no puede ser cubierta en su totalidad por los controles tecnológicos, adicionalmente se comparten las siguientes conclusiones:

- El malware dexon crea una carpeta dat e incluye archivos señuelo, con el objetivo de entorpecer y ralentizar el proceso de análisis estático, obligando a emplear una cantidad de tiempo mayor para tratar de identificar sus características.

- El método de análisis empleado, no desgasta a la organización en procedimientos extensos y complicados, su objetivo fue validar de forma rápida el comportamiento del malware y seleccionar las acciones correctivas para erradicar la infección de las máquinas y complementar los controles tecnológicos.

- Como daño colateral el malware dexon otorga permisos de administrador a todos los usuarios de la red, comprometiendo la confidencialidad, la integridad y la disponibilidad de la información. Cualquier usuario que pueda conectarse a la red tiene permisos de lectura, escritura y borrado en cualquier terminal, aumentando el nivel de riesgo para la organización.

- Realizar el análisis del malware dexon permitió evaluar el procedimiento de atención y gestión de incidentes y fue necesario modificar el flujo de actividades que permitieron reaccionar de manera contundente ante esta amenaza.

- El factor humano es una pieza clave y puede complementar los controles tecnológicos implementados por la organización, para ello es necesario capacitar constantemente a los usuarios finales en temas relacionados a malware y seguridad informática.

REFERENCIAS

[1] Figura estadística de malware, disponible en línea: https://www.av-test.org/es/estadisticas/malware/

[2] Figura implementación controles de seguridad, disponible en línea:http://www.welivesecurity.com/wpcontent/uploads/2016/04/eset-security-report-latam-2016.pdf

[3] Practical Malware Analysys. Michael Sikorski, Andrew Honig. 2012.

[4] Análisis de tráfico con wireshark, Borja Merino Febrero Inteco-Cert, 2011.

[5] Figura Análisis PUA_Dexon, disponible en línea en: https://www.trendmicro.com/vinfo/us/threatencyclopedia/malware /pua_dexon

[6] Figura elaboración propia, inicio de windows

[7] Figura elaboración propia, carpeta dat

[8] Figura elaboración propia, análisis module04.dll en virus total

[9] Figura elaboración propia, análisis wireshrak de puertos

[10] Figura elaboración propia, escaneo de recursos dexon

[11] Figura elaboración propia, copia de archivos dexon

[12] Figura elaboración propia, eliminar recursos compartidos

[13] Figura elaboración propia, eliminar reglas de firewall

[14] Figura elaboración propia, deshabilitar inicio

[15] Figura elaboración propia, eliminar llaves en el registro

[16] Figura elaboración propia, detener servicio

[17] Figura elaboración propia, regla para bloqueo de puertos

[18] Figura elaboración propia, regla para bloqueo de servicio

Autor
Juan Carlos Gamez Ramirez
Seminario de Investigación Aplicada Gestión del Riesgo